heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Labo TIB

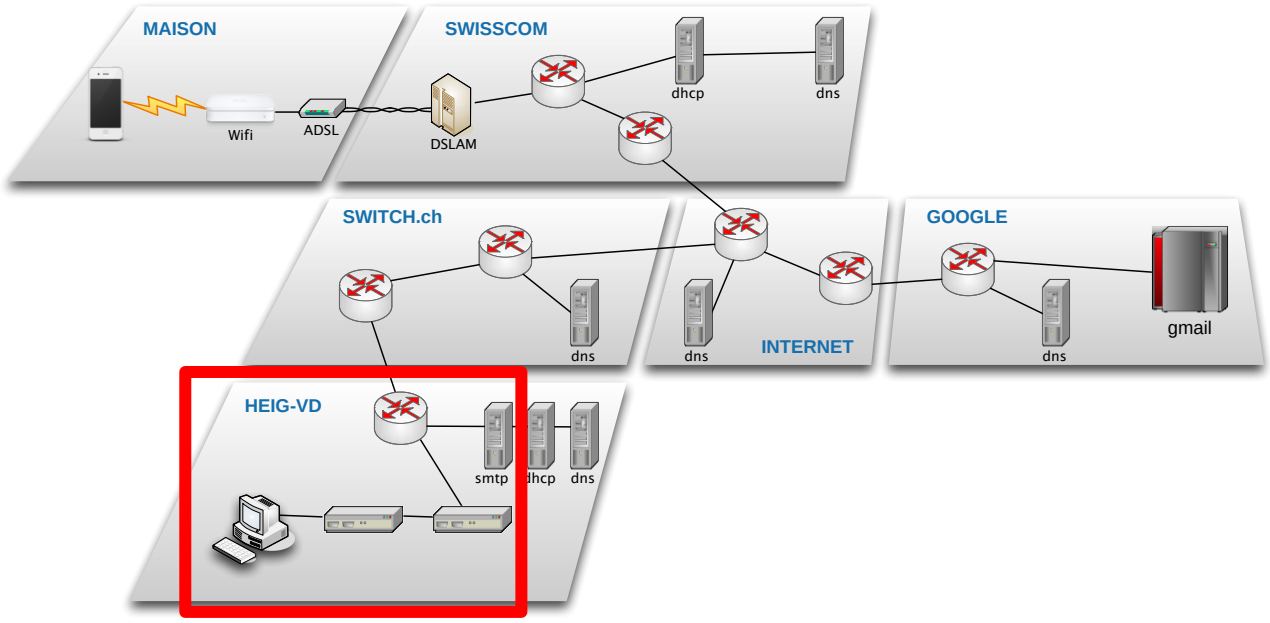
NAT

Objectifs d'apprentissage

1. Savoir effectuer des expériences réseau avec EVE-ng
2. Connaître l'interface de configuration des routeurs Cisco et savoir utiliser l'aide (point d'interrogation) et le complément automatique (tabulation).
3. Savoir expliquer le fonctionnement du NAT/PT

Contenu

Dans ce laboratoire, nous allons étudier l'utilisation d'adresses IP privées et de NAT pour la traduction entre adresses privées et adresses publiques.



1. Démarrer le simulateur GNS3
2. Configurer les adresses IP sur les machines Linux
3. Configurer le routeur Cisco.
4. Etudier le fonctionnement de NAT/PT.

Rapport à fournir

Un rapport de **2 pages au maximum** avec les éléments suivants :

1. Nom du laboratoire, noms des étudiants, date du laboratoire
2. **Objectif 1 : Configuration du réseau**
    - A l'aide du document « Annexe Cisco », expliquez le but de chacune des commandes de configuration IP du routeur Cisco.
3. **Objectif 3 : Analyse du NAT/PT**
    - Rappel de l'objectif d'apprentissage et du critère de succès.
    - Expliquez de manière succincte le fonctionnement de NAT/PT dans le scénario avec deux connexions (HEIG1-Internet1, HEIG2-Internet2). Incluez un diagramme en flèche qui montre la modification des adresses IP et des numéros de port lors du passage du NAT.
4. Auto-évaluation : est-ce que vous avez atteint les objectifs d'apprentissage de la page 1 ?

Le zip de l'export du labo est également à rendre.

Délai

Le fichier PDF du rapport et le zip du labo doivent être envoyés à l'aide du formulaire http://iict-space.heig-vd.ch/jer/rendu-labo-tib/
avant le début du prochain laboratoire.

1 Introduction

Dans les laboratoires précédents nous avons étudié la structure des adresses IP. Pour être plus précis, nous avons étudié la version 4 du protocole IP. IPv4 est encore le protocole dominant sur Internet. Il va être progressivement remplacé par son successeur IP Version 6 (IPv6) ces prochaines années.

L'introduction de IPv6 sur Internet est complexe, mais elle est nécessaire, voire de plus en plus urgente. Le problème de IPv4, la version utilisée actuellement, est le manque d'adresses. Chaque ordinateur connecté à Internet a besoin d'une adresse IP. Les adresses IPv4 ont une longueur de 32 bits. Donc, en principe, il y a plus de 4 milliards d'adresses disponibles. Mais l'allocation d'adresses IP a gaspillé beaucoup d'adresses. Un réseau classe A peut contenir plus de 16 millions d'ordinateurs. IBM dispose par exemple d'un block d'adresses classe A, mais l'entreprise est loin de nécessiter autant d'adresses.

La situation actuelle est que les adresses IPv4 vont bientôt être épuisées. Mais IPv6 n'a pas encore été déployé partout.

Depuis quelques années, il était donc nécessaire d'introduire des solutions provisoires. Les deux méthodes principales sont les adresses IPv4 privées et le NAT. Elles font l'objet de ce laboratoire.

Les plages d'adresses privées de IPv4 sont :

Classe	Adresse la plus basse	Adresse la plus haute	Nombre de réseaux	Nombre d'hôtes par réseau
A	10.0.0.0	10.255.255.255	1	16 millions
B	172.16.0.0	172.31.255.255	16	65 533
C	192.168.0.0	192.168.255.255	256	253

Dans ce laboratoire, nous allons utiliser les adresses privées 10.0.0.0/8.

2 Matériel

Dans les laboratoires précédents nous avons principalement exploré le fonctionnement des réseaux LAN et d'Internet. Aujourd'hui, pour la première fois, nous allons configurer nous-mêmes un petit réseau. C'est un nouveau défi.

Il est bien sûr possible de créer un réseau physique avec plusieurs ordinateurs, routeurs et switches. Mais votre professeur devrait vendre un de ses reins pour pouvoir acheter autant de matériel. Nous allons donc utiliser l'excellent simulateur EVE-NG qui offre en plus l'avantage que vous n'avez pas une trentaine de câbles sur votre table.

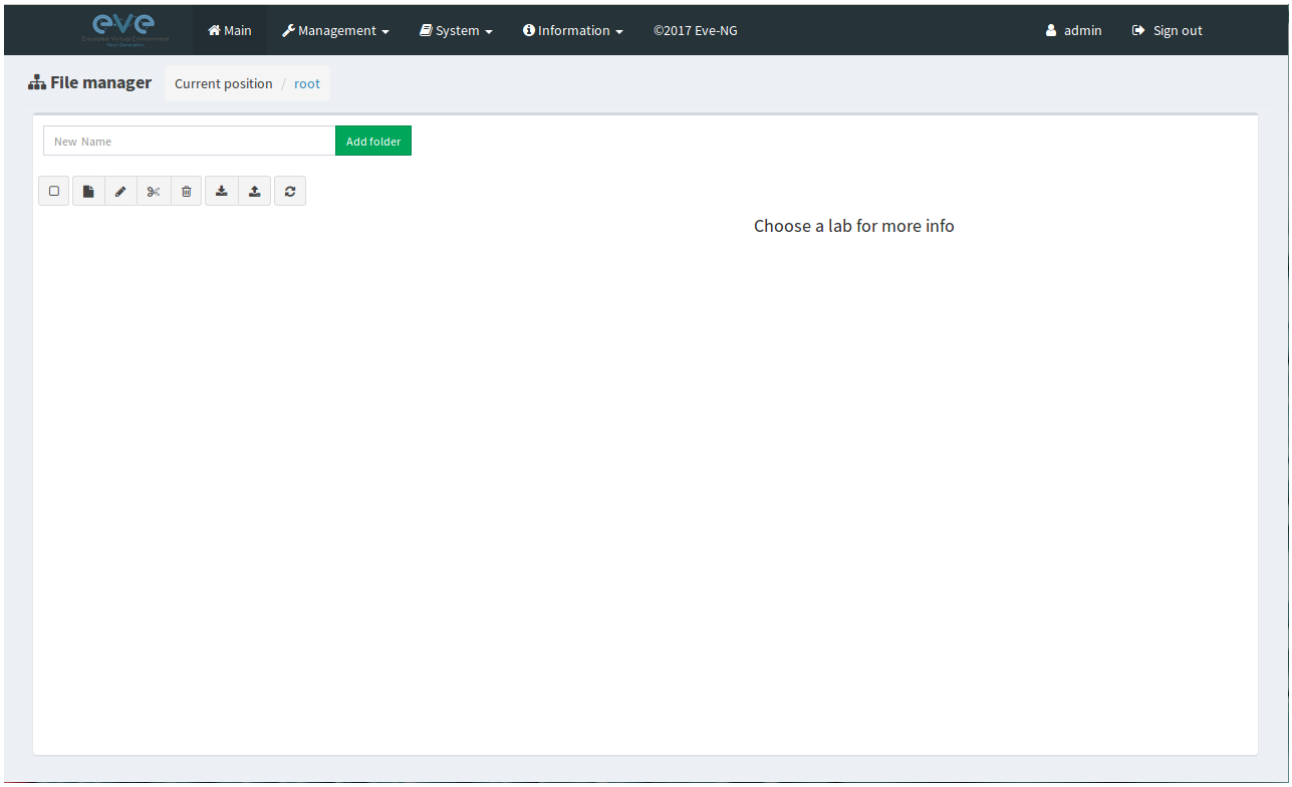
Pour utiliser EVE-NG, démarrez la machine virtuelle Linux qui vous a été fournie. EVE-NG est déjà installé.

Voici un résumé des éléments principaux de EVE-NG.

- **Démarrer la vm et loguez-vous sous labo**
- **Ouverture de Eve-ng**
  Ouvrez l'url http://127.0.01 sous Firefox
  Les identifiant sont « **admin** » « **eve** ». Sélectionnez « **Native console** »

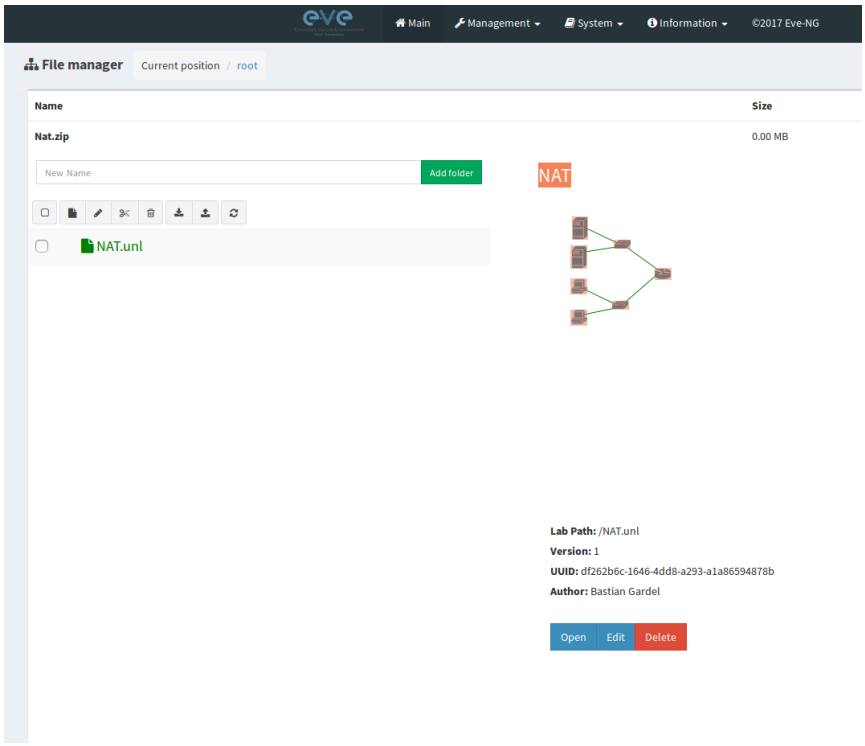
- **Importer un labo**

  Cliquez sur « **Importer** » et sélectionner le ZIP du labo. Ensuite cliquez sur « **Upload** ».



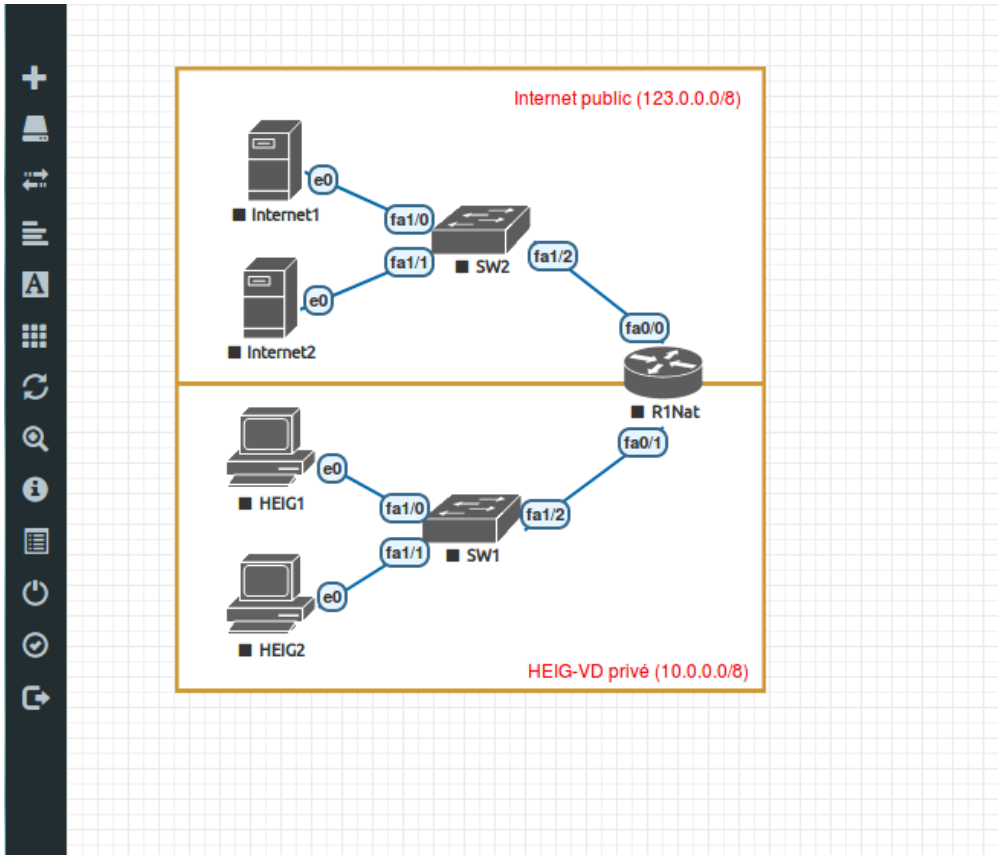
- **Ouverture du labo**

  Cliquez sur le labo et ensuite cliquez sur « **Open** »



- **Démarrer un élément**

  Faite un clic droit sur l'élément et ensuite cliquez sur « Start ». Si une erreur survient, retenter une nouvelle fois.



- **Ouvrir la console d'un élément**

  Clic gauche sur l'élément

- **Scanner une interface avec whireshark**

  Clic droit sur l'élément et puis clic sur capture. Entrez le password « **eve** ». La capture peut mettre un peu longtemps à s'ouvrir. Veuillez attendre, c'est normal.

- **Sauver la config du routeur**

  Effectuez la commande « **write** » sur en mode « **enable** » et ensuite faites un clic droit sur l'élément et cliquez sur « **Export CFG** ». **Attention !!, il faut que la console du routeur soit fermée.**

- **Editer la config d'un routeur**

  Allez sous « **Startup-Configs** » **Attention !! Il faut faire un wipe du routeur avant.**

- **Quitter le labo**
  Stoppez tous les éléments en allant sous **« More Actions – Stop all nodes »**. Puis allez sous **« More Actions – Wipe all nodes »**. (Cela assure que le routeur démarre bien avec la config sauvegardée).

Objectif 1 : Configuration du réseau

L'objectif de cette partie est de configurer les adresses IP des PCs et du routeur dans le simulateur.

L'objectif est atteint si vous pouvez envoyer des pings entre les différents PCs.

Charger le réseau

- Téléchargez l'archive zip du labo depuis le site http://iict-space.heig-vd.ch/jer, page « Labos ».
- Importez et ouvrez le labo dans EVE-ng (voir explication plus haut)
- Démarrer les éléments (voir explication plus haut)

Configuration des machines Linux

Tout d'abord il est nécessaire de configurer les adresses des machines Linux.

- Sur chacun des machines Linux du simulateur :
  - Ouvrez une console (bouton gauche). Puis tapez « Enter »
  - Loguez-vous comme utilisateur « gns3», (password : gns3)
  - Configurez l'adresse IP sur l'interface eth0 avec la commande (en remplaçant le paramètre *adresse_ip)*.

```
sudo ifconfig eth0 adresse_ip netmask 255.0.0.0
```

    Choisir des adresses 10.0.0.x/8 pour les machines du réseau HEIG-VD et des adresses 123.0.0.x/8 pour les machines Internet.
  - Configurer le routeur par défaut avec la commande

```
sudo route add default gw adresse_de_l_interface_du_routeur
```

    Cette commande indique au PC le routeur à utiliser pour atteindre d'autres réseaux que le sien.
    Utiliser l'adresse 10.0.0.1 pour ce routeur.

Configuration du routeur

Pour la première fois, nous allons configurer un routeur Cisco. Le simulateur émule un routeur physique. Il se comporte exactement comme un vrai routeur physique.

- Ouvre une console du routeur R1NAT
- Si le routeur demande « Would you like to enter the initial configuration dialog? » répondez No.
- Exécutez les commandes suivantes

```
R1Nat>enable
R1Nat#configure terminal
R1Nat(config)#interface FastEthernet0/1
R1Nat(config-if)#ip address 10.0.0.1 255.0.0.0
R1Nat(config-if)#no shutdown
R1Nat(config-if)#exit
R1Nat(config)#interface FastEthernet0/0
R1Nat(config-if)#ip address 123.0.0.1 255.0.0.0
R1Nat(config-if)#no shutdown
R1Nat(config-if)#exit
R1Nat(config)#exit
R1Nat#
```

- Effectuez des pings entre les PC. Cela doit fonctionner.

Afin de comprendre les commandes Cisco ci-dessus, lisez le document « Annexe Cisco ».

Objectif 2 : Configuration de NAT sur le routeur

L'objectif de cette partie est de configurer le NAPT sur le routeur.

L'objectif est atteint si vous pouvez envoyer des pings depuis les machines internes vers les machines externes.

Avec la configuration mise en place, les machines internes de la HEIG-VD peuvent atteindre les machines sur Internet. Mais en réalité, cette configuration ne pourrait pas fonctionner. Beaucoup de réseaux utilisent des adresses privées du type 10.x.x.x. Donc une machine sur Internet ne saurait pas comment répondre à ces adresses. On dit que les adresses IP privées ne sont pas routables sur Internet, comme le destinataire n'est pas unique.

Lorsqu'une machine HEIG-VD veut transmettre des données sur Internet, l'adresse IP privée doit être remplacé avec une adresse IP publique valable. C'est le NAT (Network Address Translation) que fait cela.

- Pour comprendre le fonctionnement de NAT, lisez le chapitre 4.4.7 du livre Kurose/Ross.
- Ensuite, configurez le NAT sur le routeur R1Nat. Plus précisément, nous allons mettre en place un NAPT (NAT avec Port Translation). Cisco appelle de type de NAT « NAT overloading ».

```
R1Nat#enable
R1Nat#configure terminal

!! Configurer le pool d'adresses et la list d'accès
R1Nat(config)#ip nat pool mypool  123.0.0.1 123.0.0.1 prefix 8
R1Nat(config)#ip nat inside source list 1 pool mypool overload
R1Nat(config)#access-list 1 permit 10.0.0.0 0.255.255.255

R1Nat(config)#interface FastEthernet0/1
!! La prochaine commande prendra un peu de temps. Patientez !
R1Nat(config-if)#ip nat inside
R1Nat(config-if)#exit

R1Nat(config)#interface FastEthernet0/0
R1Nat(config-if)#ip nat outside
R1Nat(config-if)#exit
R1Nat(config)#exit
```

Ces commandes

- définissent le pool d'adresses publiques disponibles (ici une seule adresse)
- définissent une access-list qui donne aux machines internes (10.0.0.0 –
- 10.255.255.255) le droit d'utiliser le NAT,

  - définissent les interfaces intérieure et extérieure.
- Après cette configuration, essayer de nouveau un ping entre les machines HEIG et les machines externes. Cela doit fonctionner.

Objectif 3 : Analyse du NAPT

L'objectif de cette partie est de comprendre le fonctionnement de NAPT.

L'objectif est atteint si vous savez expliquer, à l'aide d'un diagramme en flèche, comment NAPT traduit les adresses IP et numéros de port.

Nous allons tester le fonctionnement de NAT avec deux connexions, montrées ci-dessous.

HEIG1, port 32323 ←→ Internet1, port 44444

HEIG2, port 32323 ←→ Internet2, port 55555

A remarquer que HEIG1 et HEIG2 utilisent le même port source !

Nous allons utiliser l'outil Netcat (nc), afin d'établir ces outils.

- Dans Eve-ng, démarrez des captures sur les deux interfaces du routeur (voir l'explication au début du labo). Wireshark s'ouvre et affiche les paquets qui traversent cette interface.

Exécutez les commandes suivantes sur les différentes machines :

- **Internet1** : ouvrir une connexion passive (listen) sur le port 44444

```
nc -l -p 44444
```

- **Internet2** : ouvrir une connexion passive (listen) sur le port 55555

```
nc -l -p 55555
```

- **HEIG1** : se connecter au serveur 123.0.0.2, port 44444 ; utiliser le port local 32323.

```
nc -p 32323 123.0.0.2 44444
```

- **HEIG2** : se connecter au serveur 123.0.0.3, port 55555; utiliser le port local 32323.

```
nc -p 32323 123.0.0.3 55555
```

Ensuite, tout ce que vous tapez sur une console apparaît sur la machine connectée. Vous pouvez quitter les commandes avec Ctrl-C.

Pour analyser le fonctionnement de NAT/PT utiliser les outils suivants :

- Sur la console du routeur R1Nat, en mode enable, tapez la commande

```
R1Nat#show ip nat translations
```

  Elle affiche la table des traductions.

Pour comprendre NAT/PT, analysez les adresses IP et les numéros de ports des paquets sur l'interface interne et sur l'interface externe.

Puis répondez aux questions de la page 2.

!! Attention !! A la fin, n'oubliez pas de supprimer la configuration de eve-ng (Voir l'explication au début du labo).

3 Exercices avancés

***Les exercices de cette section ne sont pas obligatoires**. Ils ne seront pas considérés pour la note.*

Mais si vous avez de l'intérêt et du temps, je vous encourage à les faire, afin d'approfondir vos connaissances et apprendre encore d'avantage sur les technologies des réseaux. Dans ce cas vous pouvez joindre vos réponses aux exercices avancés au rapport de laboratoire.

Mieux connaître eve-ng

EVE-ng est un logiciel qui pourra vous être très utile tout au long de vos études. Il permet de simuler des réseaux d'ordinateurs, d'explorer des fonctionnalités en sécurité, de faire des expériences, etc. Donc je vous encourage de mieux le connaître.